

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
FORT WORTH DIVISION

HONORABLE ELAINE L. CHAO
SECRETARY, U.S. DEPARTMENT
OF LABOR

VS.

ALLIED PILOTS ASSOCIATION

§
§
§
§
§
§

CIVIL ACTION NO.4:05-CV-338-Y

ORDER DENYING PLAINTIFF'S MOTION FOR SUMMARY JUDGMENT

The above-styled and -numbered cause concerns defendant Allied Pilots Association's ("Allied") 2004 election of its national officers. The election procedures allowed for Allied's union members to vote for their national officers over the phone or through the internet. The Department of Labor ("DOL") brought this action requesting that the Court enter a judgment declaring Allied's 2004 election void and ordering a new election under DOL's supervision in accordance with the Labor-Management Reporting and Disclosure Act of 1959, 29 U.S.C. § 401, *et seq.* ("LMRDA"). The crux of DOL's complaint is that Allied's election procedures failed to ensure ballot secrecy as required by LMRDA.

I. FACTUAL BACKGROUND

The Allied Pilots Association is a national labor organization whose members are pilots employed by American Airlines, a unit of AMR Corporation. Allied's principal office is in Fort Worth, Texas, and consists of local labor organizations called "domiciles" located at each of the major pilot bases: Dallas-Fort Worth; Chicago; Miami; Washington, DC; Boston; New York City (LaGuardia); St. Louis; Los Angeles; and San Francisco.

Allied elects a national president, vice president, and secretary-treasurer for three-year terms through a referendum election administered by and under the control and supervision of the American Arbitration Association ("AAA"). For almost 50 years, AAA has been conducting elections for labor unions employing methods ranging from paper ballots and mail-in ballots to touch-screen voting machines, telephone voting, and now, internet voting. Throughout its history, AAA has conducted thousands of elections, and the association prides itself for having earned the distinction of being a reputable and neutral third-party administrator of labor-union elections.

In its 2004 election, Allied used an internet and telephone voting system ("voting system") that was designed by AAA and AAA's subcontractor, GetAGeek, Incorporated ("GAG"). AAA's and GAG's principal offices are in New York City, although GAG's director of software development, Jon Ohmann, is located in Monroe, North Carolina. AAA personnel, well versed in the statutory requirements governing labor union elections under LMRDA, worked closely with GAG to develop the voting system to be used in Allied's elections. Employees of AAA's information systems department and its elections department spent six months working with GAG to develop and test the software used in the voting system. Much of their efforts focused on ensuring its security.

The 2004 national election process began on January 16, 2004, with the opening of nominations for the three national offices. Nomination notices were mailed to union members at their last known

addresses, published in Allied's magazine, *Flightline*, and posted on union bulletin boards. Nominations were due February 6.

Prior to the voting, Allied supplied AAA with a list of its members, their addresses, and their employee identification numbers ("EIN"). AAA was responsible for designing the voting instructions and mailing those instructions to Allied's union members. AAA electronically transmitted that list to Winson Surnamer Lithography ("Winson"), which AAA employed to print the instructions and envelopes. Winson printed the voting instructions and placed them into the envelopes for mailing. AAA contracted Pitney Bowes, Incorporated ("Pitney Bowes"), to seal and mail the envelopes to Allied's union members.

To gain access to the voting system, union members needed two personal identification numbers. The first was the members' EIN. The second was a randomly generated ten-digit personal identification number ("PIN"). Winson was responsible for generating the random PINs and assigning them to the list of union members that AAA had provided. The PIN was printed on the voting instruction sheets that were mailed to Allied's members. The EIN was not printed on the instruction sheets; however, Allied published a list of its members along with their EINs on its website. Thus, any Allied member in good standing could look up another member's EIN through Allied's website.

On May 3, 2004, Pitney Bowes mailed the voting instructions and the voting system was activated. Voting was open twenty-four hours a day and ended at 4 p.m. May 24, 2004.

To vote, members accessed the voting system either by using the telephone or through the internet at the <http://www.aaaelections.org> website. AAA operated the website through its web server located in New York City, but the server neither contained nor stored any information on voters or their votes. Allied members could access the website from any computer with internet access.

Once on the website, members were required to input their EINs and PINs. That information was then transmitted, via a secure and encrypted transmission, to a computer server owned, possessed, and operated by GAG. The GAG server was protected by a firewall and was located in its New York City office. When the GAG server received the encrypted transmission entered by the member, it checked the two personal identification numbers against a database that was on the GAG server called the "member database." This database contained the member's name and two identification numbers, and was used to authenticate the voter. If the EIN and PIN submitted by the member matched the EIN and PIN on the member database, the member would be authenticated and permitted to vote.

Once authenticated, the GAG server transmitted back to the AAA website, again via a secure and encrypted transmission, an electronic ballot for the member to vote. After the member voted, that information was transmitted back, still via a secure and encrypted transmission, to the GAG server where it was stored in a separate database from the member database called the "vote database."

The GAG server contained two logs, one was the "call log" that registered when the server was accessed and recorded the internet protocol address of the computer that accessed the server. The second was the "server log" that registered what took place on the server. These logs helped GAG administrators monitor the voting activity for any suspicious activity. As GAG's Director of software, Jon Ohmann explained,

[The logs are] accurate enough from our perspective to be able to see if an abuse [sic] situation may be occurring. If we have hundreds and hundreds of requests coming from the same [internet protocol] address, it certainly raises red flags, and . . . causes us to do some further investigation. Now, it may turn out to be that it's one of these where it's a central computer and people are voting from an airport terminal or something like that, in the case of pilots, but to this point, we have never had an incident where it has even raised a red flag, let alone forced us to go and investigate a problem. Now, we do spot-check it, and we certainly check to make sure that things are as they should be, but we never had that sort of a situation. The same holds true on the telephone side as with the caller ID situation, we can track what number the phone call comes from.

Ohmann admitted that there is a drawback, however,

The assumption from the system standpoint is if you have those two pieces of information [the EIN and PIN], you're you. There's nothing on our end that can specifically say you aren't the one that's supposed to have that information, but if you have it, you're valid as far as we know.

Thus, except for registering any irregularities—such as multiple log-ons from the same internet protocol address—there was no way for the system to identify a specific and isolated instance of fraudulent

access by an individual who by some means obtained a member's EIN and PIN.

Although separate, the member and vote databases were linked together so that during the voting period, a member's vote could be connected to the member who cast that vote. Upon the initial loading of each Allied member's personal information into the member database, the GAG server automatically generated and assigned a unique and secret identifying number to each entry. This number was not the same number as the EIN or the PIN, and it was "a completely internal number" that was known only by Ohmann and other GAG personnel. After the member voted, that same number that was assigned to the entry in the member database was assigned to the member's vote entry stored in the vote database. This linked the two separate databases thereby linking members' identities with their votes.

The link between members and their votes served two purposes. First, it enabled the vote system to remove votes cast by ineligible members. After the voting closed but prior to the tallying of votes, Allied electronically supplied AAA with a complete and current list of eligible voters. AAA delivered that list to GAG, and GAG entered that list into the member database. The vote system then automatically, and without any observation, removed the votes cast by any voter who did not appear on the eligibility list that Allied provided. But this eligibility check could only be performed because the voting system was able to link voters with their votes.

The second purpose for the link was to enable members to re-log onto the voting system, view their votes, and change their votes prior to the close of elections. This was called the "change-vote feature," which could easily be disabled if Allied desired. The voting system kept a log of every instance where members re-logged onto the system and changed or resubmitted their votes. The change-vote feature could only function if the voting system were able to link voters with their votes.

At the end of the designated voting period and after the eligibility check had been performed, the voting system removed the number marker that linked voters with their votes. From that point on, it was impossible to link any votes with the voter.

During the voting period, AAA maintained a "control book" that Winson created. This book contained the names, addresses, EINs, and PINs of Allied members. The control book was locked in AAA Election Department Vice President Jeff Zaino's office at night, but was accessible "in the very back" of the AAA election office during the day. The AAA election office is a suite of offices and cubicles separated by a door from the rest of the AAA enterprise. To get to the control book, one had to pass Zaino's office and AAA Elections Department Supervisor Maria Gonzales's and AAA Elections Department Administrative Aid Linda Johnson's work spaces. Only Zaino, Gonzales, Johnson, and two temporary AAA elections workers were allowed access

to the control book.¹ Winson archived all of the information contained in the control book onto a secure, password protected, computer archive and backup CD-Rom that was accessible by a single Winson employee. Neither the control book nor the electronic backup contained any record of members' votes.

AAA used the control book for the purpose of responding to requests made by Allied members who, for whatever reason, did not have their PINs. When a member called, AAA election personnel required the member to produce numerous pieces of identifying information, including the last four digits of the member's social security number. That information was then verified with an official from Allied, and upon verification, a replacement PIN was either mailed or emailed to the requesting member.

After the votes cast in the main election were tallied, it was revealed that no candidate received a majority of votes, and therefore, a run-off election was required. The same voting system was used in the run-off election and new PINs were mailed to Allied members. The previous PINs used in the main election would not work. The voting took place between June 1 and June 22, 2004. In the run-off election, more than 6000 members cast votes and 272 members changed their votes, which was approximately 3.8% of the votes cast. Allied released the results of the election on June 22.

¹ Zaino described these two temporary workers as two long-term temporary AAA election workers with significant experience working in AAA conducted elections. Zaino explained that these two temporary workers came from a separate agency and had worked on hundreds of AAA elections over three to four years.

After the votes were tallied, Ralph Hunter was elected president, receiving 3812 votes over Mark Hunnibell, who received 2881 votes (931-vote margin of victory); Sam Bertling was elected vice president, receiving 3950 votes over Greg Shayman, who received 2722 votes (1228-vote margin of victory); and Jim Eaton was elected secretary-treasurer, receiving 3709 votes over Paul Renneisen, who received 2955 votes (754-vote margin of victory). After his defeat, Hunnibell contested the election and timely filed a complaint with Allied's appeal board in accordance with the union's internal grievances procedures.

In its constitution and bylaws, Allied has an appeal board that considers all complaints, protests, or appeals of elections. Hunnibell filed an eighteen-page, single-spaced complaint with ninety-eight pages of appendices. Although his complaint made numerous allegations of election irregularities in violation of LMRDA, only Hunnibell's allegation that the election failed to comply with the secret-ballot requirements under LMRDA is relevant here.

Hunnibell's allegation regarding the secret-ballot violation coincidentally mirrors a cautionary letter DOL sent Allied prior to its 2004 election regarding concerns with the change-vote feature used in the voting system. In fact, his complaint included a copy of that letter. Prior to the 2004 election, Allied has used a remote internet voting system substantially similar to the one employed in the 2004 election. While investigating other aspects of that system, DOL learned of the change-vote feature, and learned that in order for it

to function, the feature required members to be linked to their votes. In DOL's opinion, this violated the ballot-secrecy requirement in LMRDA.

DOL sent a letter to Richard Moyer, Allied's election administrator, detailing its concerns with the change-vote feature. After receiving that letter, Allied contacted AAA regarding DOL's concerns. AAA assured Allied that its voting system complied with the secret-ballot requirement under LMRDA.

The appeal board conducted an exhaustive investigation into Hunnibell's numerous allegations, and concluded that there was no merit to his complaint. With regards to Hunnibell's ballot-secrecy complaint, the appeal board noted that Hunnibell was the first and only member to voice any objection to the change-vote feature. The appeal board further noted that Allied had been using an electronic voting system that contained a change-vote feature since 2000—in more than 10 local domicile elections and in a previous national election. And yet, the appeal board noted, no member until now had voiced any concern regarding ballot secrecy. Thus, the appeal board concluded that Hunnibell was "over-stating the DOL's caution regarding the 'change-vote feature,'" and found it to be without merit.

After the appeal board's decision, Hunnibell timely filed his complaint with DOL. In accordance with LMRDA, DOL investigated the complaint and concluded that there was probable cause to believe that a violation of LMRDA in the conduct of Allied's 2004 election had occurred that may have affected the outcome of the election.

Specifically, DOL concluded that the change-vote feature of the voting system, because it required the system to link voters with their votes, violated the ballot-secrecy requirements under 29 U.S.C. §§ 402(k) and 481(a). Because of that link, DOL concluded that there was a possibility that it could be discovered how individual voters voted. DOL found Hunnibell's other numerous allegations meritless.

DOL found that the voting system gave certain personnel at AAA, GAG, and Winson the ability to access the voting system and ascertain how a voter had voted. In particular, DOL found that personnel at AAA, GAG, and Winson had access to the names, EINS, and PINs of Allied members. DOL concluded that their access to that information made it possible for them to log onto the voting system and ascertain how a particular member voted. And, unless the vote was actually changed, and unless that voter later re-logged onto the system to check his vote, that access would go undetected.

In addition to having access to Allied members' names, EINS and PINs, DOL also found that Ohmann had remote access to both the member and vote databases on the GAG server in New York from his home in Monroe, North Carolina, where he worked. With that access, DOL found that Ohmann could also cross-reference the internal number GAG assigned to link both the member and vote databases to determine how a particular member voted.

But after an exhaustive investigation, DOL found no specific instance where any member's vote was compromised, or any incident where any personnel from AAA, GAG, or Winson accessed the voting

system to determine how a member had voted. Further, DOL found no instance or any evidence to suggest that any Allied officer, staff member, or voter accessed the system and learned how individual voters had voted. And DOL found no evidence that anyone had misappropriated a member's EIN and PIN and used them to log onto the voting system and view that member's vote.

Moreover, during DOL's investigation, Allied conducted a survey of its members regarding the 2004 election. That survey queried whether members had re-entered the voting system for any reason, and whether they found any evidence that their vote had been tampered with. Only 110 members responded to the survey, and of the 110, only four members indicated that they re-entered the system out of concern that their votes may have been changed. But none of the four reported any vote tampering. Most who indicated that they did re-enter the system, moreover, stated that they changed their minds and thus changed their votes or, that they could not recall if they had voted and were simply checking to make sure they had in fact cast a vote.

At most, DOL's investigation found that there were a few instances where a member's PIN number was accidentally mailed to the wrong member. This occurred when the mailing machine Pitney Bowes used inadvertently glued together a few of the voting instructions mailers. This error, however, affected so few members that DOL concluded that it had no affect on the outcome of the election.

Nevertheless, DOL concluded that because the voting system employed in Allied's 2004 elections allowed for the possibility that

members could be identified with their votes, the system violated the secret-ballot requirement in LMRDA. And because, according to DOL, the compromise in ballot secrecy was a system-wide flaw, DOL concluded that its affect on the election could not be quantified. Thus, DOL concluded that it should be presumed that the system-wide breach in ballot secrecy affected the outcome of Allied's 2004 national election. Accordingly, DOL brought suit in this Court seeking a judgment declaring Allied's 2004 election void and ordering a new election under the supervision of DOL in accordance with LMRDA.

II. ANALYSIS

1. Legal Standard

Summary judgment is proper when the record establishes "that there is no genuine issue as to any material fact and that the moving party is entitled to judgment as a matter of law." FED. R. CIV. P. 56(c). An issue is considered "genuine" if "it is real and substantial as opposed to merely formal, pretended, or a sham." *Bazan v. Hidalgo Cty.*, 246 F.3d 481, 489 (5th Cir. 2001). Facts are considered "material" if they "might affect the outcome of the suit under governing law." *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248 (1986). To determine whether there are any genuine issues of material fact, the Court must first consult the applicable substantive law to ascertain what factual issues are material. *Lavespere v. Niagra Mach. & Tool Works*, 910 F.2d 167, 178 (5th Cir. 1990). Next, the Court must review the evidence on those issues, viewing the facts in the light

most favorable to the nonmoving party. *Id.*; *Newell v. Oxford Mgmt. Inc.*, 912 F.2d 793, 795 (5th Cir. 1990).

In making its determination on the motion, the Court must look at the full record including the pleadings, depositions, answers to interrogatories, admissions on file, and affidavits. See FED. R. CIV. P. 56(c); *Williams v. Adams*, 836 F.2d 958, 961 (5th Cir. 1988). Rule 56, however, "does not impose on the district court a duty to sift through the record in search of evidence to support" a party's motion for, or opposition to, summary judgment. *Skotak v. Tenneco Resins, Inc.*, 953 F.2d 909, 915-16 & n.7 (5th Cir. 1992). Thus, parties should "identify specific evidence in the record, and . . . articulate" precisely how that evidence supports their claims. *Forsyth v. Barr*, 19 F.3d 1527, 1536 (5th Cir. 1994). Further, the Court's function is not to weigh the evidence and determine the truth of the matter but to determine whether there is a genuine issue for trial. See *Anderson*, 477 U.S. at 249.

To prevail on a motion for summary judgment, the moving party has the initial burden of demonstrating that there is no genuine issue as to any material fact and that he is entitled to judgment as a matter of law. See *Celotex Corp v. Catrett*, 477 U.S. 317, 323 (1986). A moving party may submit evidence that negates a material element of the respondent's claim or defense or show that there is no evidence to support an essential element of the respondent's claim or defense. See *Celotex Corp.*, 477 U.S. at 322-24; *Crescent Towing and Salvage Co. v. M/V Anax*, 40 F.3d 741, 744 (5th Cir. 1994).

To negate a material element of the respondent's claim or defense, a moving party must negate an element that would affect the outcome of the action. *See Anderson*, 477 U.S. at 247. If the moving party alleges that there is no evidence to support an essential element of the respondent's claim or defense, the moving party need not produce evidence showing the absence of a genuine issue of fact on that essential element. Rather, the moving party need only show that the respondent, who bears the burden of proof, has adduced no evidence to support an essential element of his case. *See Celotex*, 477 U.S. at 325; *Teply v. Mobil Oil Corp.*, 859 F.2d 375, 379 (5th Cir. 1988).

When the moving party has carried its summary-judgment burden, the respondent must go beyond the pleadings and by his own evidence set forth specific facts showing there is a genuine issue for trial. *Arbaugh v. Y&H Corp.*, 380 F.3d 219, 222 (5th Cir. 2004) (citing *Celotex Corp. v. Catrett*, 477 U.S. 317, 324 (1986)); *see also* FED. R. CIV. P. 56(e). This burden is not satisfied by creating some metaphysical doubt as to the material facts, by conclusory allegations, by unsubstantiated assertions, or by only a scintilla of evidence. *See Little v. Liquid Air Corp.*, 37 F.3d 1069, 1075 (5th Cir. 1994). If the evidence is merely colorable or is not significantly probative, summary judgment may be granted. *See Anderson*, 477 U.S. at 249-50.

2. Ballot Secrecy

DOL argues that Allied's 2004 national election violated section 481(a) of LMRDA because the voting system employed compromised ballot

secrecy. The Court agrees. In light of the undisputed facts of this case, the Court concludes that the ballots were not secret within the meaning of LMRDA and DOL's regulations because during the voting period, Allied's members were required to cast their votes in a manner that linked them with their votes. This created the possibility that during the voting period members could be identified with their votes, thus making it possible that a member expressing a choice for one candidate over another could be identified with the choice expressed.

Under section 481(a), Allied is required to elect its national officers "by secret ballot among [its] members in good standing or at a convention of delegates chosen by secret ballot." 29 U.S.C. § 481(a). The Act defines a secret ballot as,

the expression by ballot, voting machine, or otherwise, but in no event by proxy, of a choice with respect to any election or vote taken upon any matter, which is cast in such a manner that the person expressing such choice cannot be identified with the choice expressed.

29 U.S.C. § 402(k). Under DOL regulations,

A prime requisite of elections regulated by [LMRDA] is that they be held by secret ballot among the members or in appropriate cases by representatives who themselves have been elected by secret ballot among the members. A secret ballot under the Act is "the expression by ballot, voting machine, or otherwise, but in no event by proxy, of a choice . . . cast in such a manner that the person expressing such choice cannot be identified with the choice expressed." . . . **The ballot must not contain any markings which upon examination would enable one to identify it with the voter.** (Emphasis added.)

29 C.F.R. § 452.97. An election by secret ballot is mandatory under the Act, and unions are responsible for taking all reasonable steps to assure ballot secrecy. See *Marshall v. Local Union 12447, United Steel Workers of America*, 591 F.2d 199, 204 (3rd Cir. 1978)(holding, "a local union is required to take all reasonable steps to assure that every voter marks his ballot in secret"); *Brennan v. Local 3489, United Steel Workers of America*, 520 F.2d 516, 522 (7th Cir. 1975)(holding ballot secrecy is mandatory and "must be assured" by the union).

The undisputed facts in this case demonstrate that the votes in Allied's 2004 election were cast in a manner that specifically identified voters with their votes. The voting system used a number identification marker to link Allied members' votes stored in the vote database with their identity stored in the member database. That in and of it self was a violation of DOL's regulation because the electronic ballot contained a marking that upon examination enabled one to identify it with the voter. But while that alone might not have compromised ballot secrecy under the statute had the system employed safeguards to prevent others from learning how members had cast their votes, what the undisputed facts reveal is that the voting system's design went to great lengths to assure its security, but failed to employ any mechanism to assure ballot secrecy.

All that was required to access the voting system was a member's EIN and PIN. The facts establish that Allied members readily had access to other members' EINs through Allied's internet website. In

other words, every members' EIN was published on Allied's website for any Allied member who had access to that website to view. Thus, from the outset, members' EINS were already compromised. Should any of Allied's members' PINs become compromised, it would be all too easy to view their votes incognito. Ohmann, GAG's software director, admitted that the system was incapable of distinguishing between a genuine user and one that had misappropriated another member's EIN and PIN. "The assumption from the system standpoint is if you have those two pieces of information, you're you, [and] . . . you're valid as far as we know." Deposition of Jon Ohmann at 90. And the facts reveal that on at least a few occasions, PINs were accidentally mailed to the wrong member.

Furthermore, countless staff from AAA, GAG, and Winson all had access to members' PINs and EINS giving them the ability to log onto the voting system at will to view how members had cast their votes. And moreover, GAG personnel with access to both the member and vote databases were also capable of identifying members with their votes because of the internal identifier used to link member entries in the member database with the member's vote in the vote database. Thus, the voting system presented a wide array of opportunities for members to be identified with their vote, thereby compromising ballot secrecy in violation of LMRDA.

While it's true that members could easily cast their votes in private, either from their telephones or their computers, the voting

system did little to assure that their votes would remain secret after they cast them.

The requirement of secrecy would seem to include not only the right to vote in secret . . . but also the right to secrecy after the ballots are cast. Any post-voting device by which it can be determined how a particular voter voted would be a violation of secrecy. (Emphasis in original.)

Bachowski v. Brennan, 413 F.Supp 147, 150 (W.D.Penn. 1976); see also *Reich v. District Lodge 720, International Association of Machinists and Aerospace Workers*, 11 F.3d 1496, 1500 (9th Cir. 1993) ("A secret ballot election is one in which it is intended that the choices made by voters will remain secret. . . . The LMRDA's secrecy mandate extends not only to the actual casting of ballots but also to any post-voting procedure designed to determine how individual union members voted or would have voted."). And neither the statute nor DOL's regulation expressly limits the ballot-secrecy requirements to union officials. Thus, it is of no moment that Allied's ballot secrecy might only be compromised by third-party neutrals.

The Court notes that more precautions were possible to prevent voter identification with their votes. First, because all Allied members had access to each other EINs, that number should not have been used because, at the outset, one of the voting system's two personal identification numbers used for security purposes had already been compromised. A better approach may have been to use members' social security numbers which, one would expect, are not as readily available to others as were their EINs. Second, after generating random PINs, the system could require members to change their PINs

once they first logged onto the system and prior to the casting of any vote.

This safeguard has one immediate, enormous benefit: neither the printing contractor that prints voter-login information sent to voters (if such a contractor is used) nor the union staff that assists in conducting the electronic election are able to log in under the guise of a given member, and view or change a vote previously cast by that member.

See Brief of Allied Union Services as Amicus Curiae Supporting Defendant Allied at 8. Thus, only the member would know the PIN necessary to log onto the voting system. Third, member identification information could be stored on a different computer than the one that stores a member's vote, instead of just on different databases on the same computer. While a marker could still be used to link voters with their votes, the system could be designed so that no computer software engineer would have access to both computer systems thereby preventing any possibility of exploitation of the electronic marker to learn how members had cast their votes. See *Id.* at 8-9. Thus, voter secrecy would remain assured. And finally, while members could be allowed to re-login to change their votes, members could be precluded from viewing their previous votes. Thus, should a member's identification become compromised, an unauthorized user would still be prevented from viewing how the member voted. Allied's voting system came up short in implementing any of these measures to assure ballot secrecy.²

² The Court in no way intends to imply that had Allied incorporated all or any of the listed measures that its voting system would have satisfied the ballot-secrecy requirements of LMRDA and DOL regulations. Nor does the Court intend to imply that any other voting system that employs these measures would satisfy the statutory and regulatory requirements. Rather, the Court simply means to demonstrate how woefully

Without a doubt, electronic voting carries with it great advantages. Its mere convenience will probably contribute greatly to increased voter turnout.³ It's cost effective and efficient—the vote is paperless and the final vote count is instantaneous. Its pinpoint accuracy will eliminate any question regarding voter intent on ballots ambiguously or incorrectly marked. And with the appropriate safeguards in place, its security is nearly impenetrable. While these are surely all benefits that electronic voting can provide, they cannot be allowed to come at the price of that fundamental principle crucial in any truly democratic election—ballot secrecy.

Congress's principle purpose in LMRDA was to mandate a set of rules designed "to ensure free and democratic elections." *Wirtz v. Hotel, Motel & Club Employees Union, Local 6*, 391 U.S. 492, 496 (1968).

A pervasive theme in the congressional debates about the election provisions was that revelations of corruption, dictatorial practices and racketeering in some unions investigated by Congress indicated a need to protect the rights of rank-and-file members to participate fully in the operation of their union through processes of democratic self-government, and, through, the election process, to keep the union leadership responsive to the membership.

Id. at 497. This theme of ensuring democratic self-government that is responsive to the needs of union members is reflected in the very

short Allied's voting system comes to assuring ballot secrecy by illustrating plausible techniques that are currently in use that would have made a greater impact on assuring ballot secrecy.

³ The Court does note that Allied has not supplied the Court with any evidence that since it started using electronic voting, voter turnout has greatly increased.

mandates of the statute: National elections must be held at least once every five years and local elections at least once every three years; all union members in good standing must be allowed to seek office subject to reasonable qualifications; the union is prohibited from discriminating in favor of one candidate or against another candidate and must insure equality of treatment in campaigning; and, of course, the union must assure ballot secrecy. See 29 U.S.C. § 481(a)-(e). Thus, the uncertainty of ballot secrecy that characterized Allied's latest election cannot be countenanced in light of Congress's clear intent expressed in the statute.

3. Affect on the Outcome of the Election

DOL maintains that because the lack of assurance of ballot secrecy was a system-wide failure, the extent of the breach "cannot be quantified or cured." DOL contends that "it is impossible to determine" whether fears or concerns regarding ballot secrecy affected how voters actually voted or affected whether a member decided to cast a vote. Thus, DOL argues that "the presumption must be that the outcome was affected, and the tainted election must be re-run under the supervision of the DOL." The Court disagrees.

Section 482(c) of LMRDA states,

If, upon a preponderance of the evidence after a trial upon the merits, the court finds . . . that the violation of section 481 of this title may have affected the outcome of an election, the court shall declare the election, if any, to be void and direct the conduct of a new election under supervision of the Secretary

Thus, DOL is not entitled to a judgment declaring Allied's 2004 national election void and ordering a new election under DOL's supervision unless it is shown that the breach of ballot secrecy "may have affected" the outcome of the election. See *Local 6*, 391 U.S. at 505.

In *Local 6*, the Supreme Court held that proof of a violation of LMRDA has "the effect of establishing a prima facie case that the violation 'may have affected' the outcome." *Id.* at 506-7. In essence, mere proof of a violation of LMRDA creates a presumption that the violation may have affected the outcome of the election. This presumption, however, may be rebutted "by evidence [that] supports a finding that the violation did not affect the result." *Id.*

In *Marshall v. Local 468, International Brotherhood of Teamsters, Chauffeurs, Warehousemen, and Helpers of America*, the United States Court of Appeals for the Ninth Circuit held that the determination of whether a violation of LMRDA may have affected the outcome of an election was "not susceptible to determination by summary judgment." 643 F.2d 575, 578 (9th Cir. 1980). The Court agrees. While the determination of whether the voting system employed in Allied's 2004 national election violated the ballot-secrecy requirement in LMRDA is a legal question, the Court concludes that the determination of whether such violation may have affected the outcome of the election is a question of fact. Thus, where, as here, the union has presented some genuine, tangible, and probative evidence to rebut the presump-

tion that the violation of LMRDA may have affected the outcome of the election, summary judgment is not appropriate.

Here, Allied has presented evidence that it has been using this same voting system since 2000 in at least 10 local elections and one previous national election. Allied's evidence shows that up until the 2004 election, no member had lodged any complaint concerning the voting system's ability to maintain ballot secrecy. Furthermore, Allied conducted a survey of its members designed to elicit any concerns regarding ballot secrecy in the 2004 elections. Of the more than 6000 members that voted, only 110 bothered to fill out any of the surveys and, of the 110, merely four reported hearing rumors that their votes could have been compromised. Contrary to DOL's assertion, this is tangible and probative evidence that members did not have concerns regarding the secrecy of their cast ballots. Coupling that with evidence that since the employment of electronic voting in 2000, voter turnout has substantially increased, Allied could present a compelling case to the jury that there was no affect on the outcome of the 2004 national election.


Additionally, two exhaustive investigations by Allied and DOL into the issue of ballot secrecy unveiled not a single instance where a member had been identified with his vote, and not a single instance of vote tampering. Moreover, the complaint as to ballot secrecy that has culminated in the filing of this case came not from a regular voting member of Allied, but from one of the candidates who lost the election. Hunnibell's complaint did not list any factual allegations

that members' votes were actually compromised or that any member had claimed that a concern regarding the secrecy of balloting impacted how, or if, he voted. Instead, Hunnibell's complaint simply piggybacked on DOL's letter to Allied sent prior to its 2004 national election detailing its concern regarding the change-vote feature and how it might compromise ballot secrecy. In essence, it was simply another allegation lodged in connection with numerous other allegations with the hope that one will succeed in invalidating the election. All this taken together raises a genuine issue of material fact regarding whether the violation of the ballot-secrecy requirement may have affected the outcome of the election. See *Local 6*, 391 U.S. at 508 (Holding union is required to present "tangible evidence against the reasonable possibility that the [violation] . . . did affect the outcome" and not rest on pure conjecture). Had Allied failed to present any tangible evidence that its failure to assure ballot secrecy in its 2004 national election did not affect the outcome of the election, DOL could properly rely on the presumption that a violation of LMRDA in the conduct of a union election may have affected the outcome of the election. And, under that circumstance, summary judgment would be proper. Cf. *Local Union 12447*, 591 F.2d at 206 (relying on presumption that violation of ballot-secrecy requirement may have affected outcome of election because "the union offered no evidence to rebut this showing"). Thus, DOL has failed to carry its burden to establish its entitlement to judgment as a matter of law.

III. CONCLUSION

The Court holds that the voting system employed in Allied's 2004 national election violated sections 402(k) and 481(a) because it failed to assure voting by secret ballot. Furthermore, the Court holds that the question of whether of violation of LMRDA may have affected the outcome of an election is a question of fact normally not appropriate for determination by summary judgment. Finally, because Allied has presented genuine, tangible, and probative evidence to rebut the presumption that the violation of LMRDA may have affected the outcome of the election, Allied has satisfied its burden of establishing a genuine issue for trial. Accordingly, DOL's motion for summary judgment (doc. #23) is DENIED.

SIGNED February 20, 2007.



TERRY R. MEANS
UNITED STATES DISTRICT JUDGE